

**REMARKS**

Claims 1 and 3-33 are currently pending in the subject application and are presently under consideration. Claims 1, 20, 24, 28 and 29 have been amended as shown on pp. 1 and 4-7 of the Reply.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

**I. Rejection of Claims 1, 5-7, 9, 10, 20, 23-25 and 27-29 Under 35 U.S.C. §103(a)**

Claims 1, 5-7, 9, 10, 20, 23-25 and 27-29 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Spriggs, *et al.* (US 6,421,571) in view of Abraham (US 5,539,906). It is requested that this rejection be withdrawn for at least the following reasons. Spriggs, *et al.* and Abraham taken alone or in combination do not teach or suggest every element of the claimed invention, and further, one ordinarily skilled in the art could not combine these references to successfully implement the claimed invention.

To reject claims in an application under §103, an examiner must establish a *prima facie* case of obviousness. A *prima facie* case of obviousness is established by a showing of three basic criteria. First, there *must be some suggestion or motivation*, either in the references themselves or in the knowledge generally available to *one of ordinary skill in the art, to modify the reference or to combine reference teachings*. Second there must be a *reasonable expectation of success*. Finally, the prior art reference (or references when combined) *must teach or suggest all the claim limitations*. See MPEP §706.02(j). The *teaching or suggestion to make the claimed combination* and the reasonable expectation of success *must be found in the prior art and not based on the Applicant's disclosure*. See *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991) (emphasis added).

The claimed subject matter generally relates to a system that automates security in an industrial control environment by automatically creating security profiles for industrial automation devices in the environment and enforcing these profiles with respect to accessing entities. Such profiles may define different levels of access for various entities. To this end, independent claim 1 recites an automation security system, comprising: an asset component that defines an industrial automation device; an access component that

defines a security attribute associated with the industrial automation device, the security attribute including a location attribute and **a time attribute that grants access to the asset component for a predetermined amount of time**; and a security component that regulates access to the industrial automation device based upon the security attribute. Spriggs, *et al.* and Abraham, when taken alone or in combination, fail to teach or suggest every element of the claimed invention.

Spriggs *et al.* discloses a system for that includes a unified display environment and a common database structure for protecting and managing industrial plant assets. (Col. 3, lns. 20-25). Spriggs *et al.* also discloses using a security manager module that provides configuration security settings for the system wherein the security is configured based on the logged-in user and certain tasks, such as editing set points or acknowledging events. (Col. 27 ln. 64 - Col. 28 ln. 1). Abraham discloses a data processing system for controlling data security in a data processing system. (Col 2, lns. 47-50). Further, Abraham discloses that user groups which access data are located at a plurality of locations, and a copy of selected database elements is associated with each location. (Col. 3, lns. 17-20). Abraham also discloses that access will be denied to a user based on the status of the data and the location of the user. (Col. 3, lns. 20-22). Moreover, Abraham discloses that a manufacturing engineer, for example, at a particular location can only access a copy of the design data which is associated with that particular location. (Col. 3, lns. 22-25).

The Examiner acknowledges that Spriggs *et al.* does not specifically disclose the security attribute including a location attribute and offers Abraham to cure this deficiency. However, neither Spriggs *et al.* nor Abraham teach, disclose or suggest that the security attribute including a location attribute **and a time attribute that grants access to the asset component for a predetermined amount of time**, as the amended claim 1 now recites.

Amended independent claim 20 recites an automation security system, comprising: a server that manages a network interface between networked industrial automation devices and other devices attempting access to the networked industrial automation devices; and a security management module associated with the network interface that enforces an enterprise wide policy and that manages security threats

directed to the networked industrial automation devices, the enterprise wide policy including a location attribute and *a time attribute that limits access to the networked industrial automation devices to certain time periods*. Spriggs, *et al.* and Abraham, when taken alone or in combination, fail to teach or suggest every element of the claimed invention.

Spriggs *et al.* discloses a system that includes a unified display environment and a common database structure for protecting and managing industrial plant assets. (Col. 3, lns. 20-25). Spriggs *et al.* also discloses the system is capable of correlating information from multiple sources that allows timely, operational decisions on machinery condition that consider both the machinery and the surrounding process conditions/constraints (Col. 2, lns. 27-31). However, Spriggs *et al.* is silent regarding limiting access to the plant assets *to certain time periods*. Likewise, Abraham is also silent to such novel aspects.

Amended independent claim 24 recites an automation security methodology, comprising: electronically analyzing an industrial automation device; programmatically modeling the industrial automation device in accordance with network security considerations, the network considerations include a location attribute and *a time attribute that controls if and how long network access is granted to the industrial automation device*; and automatically developing a security framework for an automation system based in part on the modeling of the industrial automation device and a network access type. Spriggs, *et al.* and Abraham, when taken alone or in combination, fail to teach or suggest every element of the claimed invention.

Spriggs *et al.* discloses that the system includes a security manager module that provides configuration security settings for the system wherein the security is configured based on the logged-in user and certain tasks, such as editing set points or acknowledging events (Col. 27, ln. 64 through Col. 68, ln. 4). Additionally, Abraham discloses granting security access to users based on the status and location of the users (Col. 3, lns. 17-25). However, neither Spriggs *et al.* nor Abraham teach, disclose or suggest that the network considerations include *a time attribute that controls if and how long network access is granted to the industrial automation device*.

Amended independent claim 28 now recites an automated security system for an industrial control environment, comprising: means for defining one or more security

attributes associated with at least one network request, the security attributes include *at least one of: a location attribute, a time attribute, a role attribute, and an access type attribute*; means for processing the one or more security attributes; means for automatically determining which network devices require security resources; and means for controlling access to at least one of a network device and the industrial automation component based in part on the one or more security attributes. Spriggs, *et al.* and Abraham, when taken alone or in combination, fail to teach or suggest every element of the claimed invention.

For example, as depicted in the specification for the claimed subject matter, a security model can include asset and access based models having respective security attributes that describe the type of automation component to be accessed and the type of access permitted within the automation component such as a read and/or write access. (Pg. 6, Ins. 7-12). Further, the specification for the claimed subject matter discloses that the security models can include role information or attributes relating to the users who attempt access (*e.g.*, Manager, Engineer, Maintenance) and can include a time-coded attribute limited entry to a device to a specified time. (Pg. 3, Ins. 27-29 and Pg. 17, ln. 27). Spriggs *et al.* discloses a system wherein the security is configured based on the logged-in user (Col. 27, Ins. 65-67). However, Spriggs *et al.* is silent in regards to *a location attribute, a time attribute, a role attribute, or an access type attribute* in reference to the security configuration. Abraham discloses granting security access to users based on status and locations of the users (Col. 3 Ins. 17-25). Further, Abraham discloses a security level that can be based on granting access to different security groups. (Col. 7, Ins. 1-5). However, Abraham does not teach or suggest using a security attribute based on *a time attribute, a role attribute, or an access type attribute*.

Amended claim 29 recites a security schema for a factory automation system, comprising: a first data field that describes industrial automation devices; a second data field that describes security parameters for the industrial automation devices, the security parameters including a location attribute and a *time attribute that enables access to the industrial automation devices for a specified time*; and a schema that associates the first and second data fields, the schema employed to limit access to the industrial automation devices based upon the security parameters. However, in view of the arguments

presented for amended independent claims 1, 20, 24, and 28, similarly neither Spriggs *et al.* nor Abraham teach or suggest including a *time attribute that enables access to the industrial automation devices for a specified time* as part of the security parameter.

In view of at least the foregoing, it is readily apparent that Spriggs *et al.* even in light of Abraham fails to teach, disclose or suggest each and every element recited in the subject claims. Therefore, the rejection of claims 1, 20, 24, 28, and 29 (and associated dependent claims 5-7, 9, 10, 23, 25, and 27) should be withdrawn.

## **II. Rejection of Claims 3, 4, 11-19, 21-22, 26 and 30-33 Under 35 U.S.C. §103(a)**

Claims 3, 4, 11-19, 21-22, 26, and 30-33 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Spriggs *et al.* in view of Le Saint (US 2004/0034774). It is respectfully requested that this rejection be withdrawn for at least the following reasons. Spriggs *et al.* and Le Saint, when taken alone or in combination, fail to teach or suggest all elements recited in the subject claims. In particular, Le Saint fails to make up for the aforementioned deficiencies with respect to claims 1, 20, 24, 28 and 29, from which claims 2-4, 11-19, 21-22, 26, and 30-33 depend. Accordingly, it is respectfully requested that the rejection of these claims be withdrawn.

**CONCLUSION**

The present application is believed to be in condition for allowance in view of the above comments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [ALBRP303USA].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/

Himanshu S. Amin

Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP  
24<sup>TH</sup> Floor, National City Center  
1900 E. 9<sup>TH</sup> Street  
Cleveland, Ohio 44114  
Telephone (216) 696-8730  
Facsimile (216) 696-8731